CHEAT SHEET

Seguridad en Microsoft 365 Copilot

Enfocado en IA

Este Cheat Sheet resume las acciones esenciales para asegurar tu entorno de Microsoft 365 antes de implementar Copilot o Agentes. Incluye medidas de autenticación, control de accesos, clasificación de datos, políticas de compartición, revisión de fuentes de conocimiento, monitoreo y capacitación de usuarios. Su objetivo es minimizar riesgos, proteger la información y garantizar que Copilot opere sobre una base segura y confiable.

1) Autenticación y control de acceso

- Activa MFA (autenticación multifactor) para todos los usuarios, sin excepciones.
- Configura acceso condicional para limitar Copilot a dispositivos y ubicaciones autorizadas.
- Revisa y aplica políticas de contraseñas seguras (longitud, complejidad, bloqueo tras intentos fallidos).
- Habilita cierre automático de sesión tras un periodo de inactividad.
- Elimina o desactiva cuentas inactivas o sin propietario claro.

2) Revisión y ajuste de roles

- Aplica el principio de mínimo privilegio para acceso a configuración y administración de agentes.
- Usa roles granulares para separar tareas de configuración, contenido y supervisión.
- Revisa roles en Microsoft Entra ID periodicamente usuarios y aplicaciones.
- Documenta quién tiene privilegios elevados y por qué.
- Elimina accesos temporales una vez cumplida la tarea.

3) Limpieza y clasificación de datos

- Depura contenido obsoleto en SharePoint. Instruye a tus colaboradores para hacer lo mismo en OneDrive
- Elimina documentos duplicados o sin uso.
- Aplica etiquetas de sensibilidad a información crítica.
- Configura DLP (Data Loss Prevention) para prevenir filtraciones.
- Centraliza fuentes de información para evitar que Copilot use contenido no validado.

4) Políticas de compartición y permisos

- Limita la compartición externa a dominios aprobados.
- Configura caducidad automática de enlaces compartidos.
- Revisa permisos heredados en bibliotecas y carpetas.
- Bloquea la descarga de documentos sensibles.
- Habilita alertas cuando un documento sensible se comparte externamente

5) Seguridad en las fuentes de conocimiento

- Valida que el contenido sea exacto, actualizado y seguro antes de que Copilot lo use.
- Clasifica y etiqueta documentos según su nivel de sensibilidad.
- Protege información personal o confidencial con encriptado y permisos.
- Elimina contenido irrelevante o desactualizado de las fuentes conectadas.
- Mantén un repositorio maestro revisado periódicamente.

6) Monitoreo y auditoría

- Activa Microsoft Purview Audit para rastrear interacciones con Copilot.
- Configura alertas para actividades críticas o inusuales.
- Revisa registros de acceso y cambios de configuración semanalmente.
- Monitorea la exportación masiva de datos.
- Documenta incidentes y acciones correctivas.

7) Entrenamiento seguro de usuarios

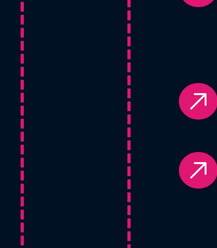
- Capacita en privacidad, seguridad y uso responsable de Copilot.
- Explica qué datos pueden o no incluirse en prompts.
- Entrena sobre detección de phishing y ataques de ingeniería social.
- Promueve la verificación de datos antes de compartirlos.
- Publica una guía interna con buenas prácticas y reglas claras.

8) Seguridad Exchange Online y Teams

- **Configura la Seguridad de Firmas de Correo: DKIM y DMARC**
- Configura Safe Links y Safe Attachments en Defender for Office 365 para bloquear amenazas en correos y chats.
- Activa políticas de retención según requisitos legales o de negocio.
- Restringe la creación de equipos y canales en Teams solo a usuarios autorizados.
- Supervisa el uso de conectores y aplicaciones de terceros en Teams para evitar filtraciones de datos.

Conclusiones

- La seguridad es un prerrequisito, no un extra, para Copilot.
- Un entorno limpio y controlado reduce riesgos y mejora la calidad de resultados.
- La gobernanza continua es más efectiva que las revisiones puntuales.
- El factor humano es tan importante como la tecnología.
- Copilot y los Agentes solo aportan valor si operan sobre una base segura y confiable.



Sígue a 👉 @gilerika en LinkedIn

SUSCRÍBETE A MI NEWSLETTER
ERIKA AUTOMATED